Technical Update for May 15:

- CISA has released an analysis report, AR21-134A Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise. The report provides detailed steps for affected organizations to evict the adversary from compromised on-premises and cloud environments. Additionally, CISA has publicly issued Emergency Directive (ED) 21-01 Supplemental Direction Version 4: Mitigate SolarWinds Orion Code Compromise to all federal agencies that have—or had—networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity. Although the guidance in AR21-134A and ED 21-01 Supplemental Direction V.4 is tailored to federal agencies, CISA encourages critical infrastructure entities; state, local, territorial, and tribal government organizations; and private sector organizations to review and apply it, as appropriate. Note: the U.S. Government attributes this activity to the Russian Foreign Intelligence Service (SVR). Additional information may be found in a statement from the White House and in the three Joint Cybersecurity Advisories summarized in the CISA Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise.

Technical Update for April 27:

- FBI, DHS, and CISA released a joint alert titled Alert AA21-116A: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders that covers trending attack methods used by the SVR and mitigation techniques that network defenders can take to protect their organizations. This alert comes in response to a recent statement released by the White House that attributes the SolarWinds compromise to the SVR. Since 2018, the FBI has observed the SVR’s targeting of cloud resources to obtain information, and the SolarWinds compromise reflects the continuance of that trend. The alert identifies common TTPs used by the SVR including password spraying, zero-day vulnerability exploitation, and the use of the WELLMESS malware. The alert also provides mitigations for each TTP, such as: enabling multi-factor authentication, strengthening passwords, and auditing logs for any suspicious activities.

- CISA and NIST have released a new inter-agency resource to assist software vendors and customers with defending their organizations against supply chain attacks. The resource provides an overview of software supply chain risks, and provides recommendations for how to use the NIST Cyber Supply Chain Risk Management (C-SCRM) Framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate software supply chain risks.
Technical Update for April 19-23:

- CISA released an analysis report titled *Analysis Report (AR21-112A): CISA Identifies SUPERNOVA Malware During Incident Response* which describes how a threat actor gained initial entry into a victim's systems by masquerading as teleworking employees and connecting to the Pulse Secure VPN appliance. Once authenticated, the threat actor moved laterally to the SolarWinds Orion appliance where they installed SUPERNOVA before dumping and exfiltrating credentials.

SUPERNOVA is a malicious web shell backdoor that allows a remote operator to inject code and is used to perform reconnaissance, conduct domain mapping, and steal sensitive information and credentials. According to SolarWinds, SUPERNOVA is not embedded within the Orion platform as part of the original supply chain attack but is designed to appear as part of the SolarWinds product and placed on a system that hosts SolarWinds Orion. CISA assesses that the threat actor responsible for SUPERNOVA differs from the actor responsible for the original SolarWinds supply chain compromise and advises organizations that find SUPERNOVA on their systems to treat the incident as a separate attack. The analysis report provides TTPs observed by CISA during analysis as well as some general recommendations for strengthening the overall security posture.

Technical Update for April 12-16:

- CISA and the Department of Defense Cyber National Mission Force (CMNF) have announced that additional analysis of the SolarWinds-related malware has led to the discovery of two new variants: SUNSHUTTLE and SOLARFLARE. The report, *MAR-10327841-1.v1 (AR21-105A)*, contains detailed analysis of 18 malicious samples and artifacts that are directly related to the SolarWinds compromise. The analyzed files include configuration files, script files that manipulate Windows registry keys, and the China Chopper web shell file. The China Chopper web shell, in particular, provides threat actors with alternative means of accessing a compromised network, even when the infection was remediated. CISA also encourages users and administrators to review U.S. Cyber Command’s VirusTotal page.

Technical Updates for April 5-9:

- CISA announced the release of a Splunk-based dashboard called *Aviary* which was developed to visualize and analyze outputs from the Sparrow detection tool that was released in December. Sparrow was designed to support hunts for SolarWinds-related threat activity and Aviary works in tandem with Sparrow to facilitate analysis of the output. CISA also updated *Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments* to include directions on how to install and use the Aviary dashboard in conjunction with the Sparrow tool.

Technical Updates for March 15-19:

- CISA announced the development of a forensics collection tool called *CHIRP (CISA Hunt and Incident Response Program)*. The tool was designed to assist network defenders in finding indicators of compromise (IOCs) associated with the SolarWinds and Active Directory/M365 compromise. The tool is freely available on CISA’s GitHub repository. The tool operates similarly to the Sparrow tool in that it scans for signs of APT compromise within the on-premise
environment. CISA advises organizations to use the CHIRP tool to examine Windows event logs and registry, query network artifacts, and apply YARA rules to detect malware backdoors or implants. The announcement does contain a link to an alert that provides more technical details on how to operate CHIRP.

- CISA has released a table of tactics, techniques, and procedures (TTPs) used by the advanced persistent threat (APT) actor involved with the recent SolarWinds and Active Directory/M365 compromise. The table uses the MITRE ATT&CK framework to identify APT TTPs and includes detection recommendations. This information will assist network defenders in detecting and responding to this activity. CISA encourages network defenders to review SolarWinds and AD/M365 Compromise: Detecting APT Activity from Known TTPs and implement the recommendations.

- Cloud E-mail Security provider Mimecast published their forensic investigation with Mandiant and have eliminated the threat actor's access to their environment. During Mimecast's investigation, they learned that the threat actor used the SolarWinds supply-chain compromise to gain access to part of their production grid environment. Using this entry point, the threat actor accessed certain Mimecast-issued certificates and related customer server connection information. The threat actor also accessed a subset of email addresses and other contact information, as well as encrypted and/or hashed and salted credentials. In addition, the threat actor accessed and downloaded a limited number of our source code repositories, but Mimecast found no evidence of any modifications to their source code nor do they believe there was any impact on our products. Mimecast also found no evidence that the threat actor accessed email or archive content held on behalf of their customers.

**Technical Updates for March 8-12:**

- Since December 2020, CISA has been responding to a significant cybersecurity incident involving an advanced persistent threat (APT) actor targeting networks of multiple U.S. government agencies, critical infrastructure entities, and private sector organizations. The APT actor added malicious code to multiple versions of the SolarWinds Orion platform and leveraged it—as well as other techniques, including—for initial access to enterprise networks. After gaining persistent, invasive access to select organizations’ enterprise networks, the APT actor targeted their federated identity solutions and their Active Directory/M365 environments. CISA has published two new resources on the follow-on activity from this compromise:
  
  o The Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise web page to provide actionable guidance to organizations affected by this APT activity. Although the guidance on the web page is directed to federal departments and agencies, CISA encourages affected critical infrastructure and private sector organizations to review and apply it, as appropriate.
  
  o The CISA Insights: SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders supports executive leaders of affected organizations in understanding the threat, risk, and associated actions they should take in response to the APT activity. The CISA Insights specifically applies to organizations with affected versions of SolarWinds Orion who have evidence of follow-on threat actor activity.

- CISA encourages affected organizations to review and apply the necessary guidance in the Remediating Networks Affected by the SolarWinds and Active Directory/M365
Technical Updates for March 1-5:

- Microsoft Threat Intelligence Center (MSTIC) released a blog post outlining three new pieces of malware identified as being used by the threat actors responsible for the SolarWinds hack. Additionally, Microsoft is revising their naming convention for the actor behind the attacks against SolarWinds, the SUNBURST backdoor, TEARDROP malware, and related components as NOBELIUM. According to Microsoft, these new malware strains—in use from August to September 2020—were tailored for specific networks and seem to be introduced after the actor gained access through compromised credentials or the SolarWinds binary and moving laterally. The names of the tools are GoldMax, Sibot, and GoldFiner.
  - GoldMax acts as a command-and-control backdoor for the actor. It resides on the network as a scheduled task impersonating systems management software. The tool establishes a secure session key to communicate with the C2. Once connected, the C2 can send commands to be launched for various operations.
  - Sibot is a dual-purpose malware designed to achieve persistence on the infected machine and then download and execute a payload from a remote C2 server. The script file is given a name that impersonates legitimate Windows tasks and is stored either in the registry or in an obfuscated format on disk. The script is then run by a scheduled task.
  - GoldFinder is most likely a custom HTTP tracer tool that logs the routes or hops that a packet takes to reach a hardcoded C2 server. When launched, the malware issues an HTTP server request for a hardcoded IP address and logs the HTTP response to a plaintext log file. The tool can identify all HTTP proxy servers and other redirectors such as network security devices that an HTTP request travels through inside and outside the network to reach the intended C2 server. When on a compromised device, the tool can be used to notify the actor of potential points of discovery or logging of their other actions such as C2 communication with GoldMax.

- FireEye released a blog post identifying a new backdoor called SUNSHUTTLE that seems to have originated from a US-based entity in August 2020. SUNSHUTTLE is a second-stage backdoor that features some detection evasion capabilities and may be linked to the threat actors (referred to as UNC2452) responsible for the SolarWinds hack. SUNSHUTTLE reads a local or embedded configuration file, communicates with a hard-coded C2 server over HTTPS, and supports commands including remotely uploading its configuration, file upload and download, and arbitrary command execution. One of the FireEye authors confirmed on Twitter that SUNSHUTTLE and GoldMax are the same strand of malware.

- In a blog post, Microsoft publicly released the CodeQL queries they used to analyze their own source code at scale in order to rule out the presence of the code-level indicators of compromise (IoCs) and coding patterns associated with Solorigate. In the blog post, Microsoft detailed that sourcing the CodeQL queries they used in this investigation so that other organizations may perform a similar analysis. Note that the queries covered in the blog serve to home in on source code that shares similarities with the source in the Solorigate implant, either
in the syntactic elements (names, literals, etc.) or in functionality. Both can occur coincidentally in benign code, so all findings should be reviewed to determine if they are actionable. Additionally, there is no guarantee that the malicious actor is constrained to the same functionality or coding style in other operations, so these queries may not detect other implants that deviate significantly from the tactics seen in the Solorigate implant. Per Microsoft, these should be considered as just a part in a mosaic of techniques to audit for compromise. Finally, the Solorigate-Readme.md contains detailed descriptions of each query and what code-level IoCs each one is attempting to find. It also contains guidance for other query authors on making adjustments to those queries or authoring queries that take a different tactic in finding the patterns.

Technical Update for February 15-19:

- Microsoft released a final update on their internal Solorigate investigation. Findings indicate that there was no evidence of access to production services or customer data. Furthermore, there were no indications that Microsoft systems were used to attack other victims. The company praised their defense-in-depth protections as the reason the threat actors were not able to gain access to privileged credentials or leverage SAML techniques. The update also shed more light on the source code repositories that the threat actors accessed. Microsoft identified the repositories contained code for “a small subset” of Azure components, Intune components, and Exchange components.
- Microsoft accompanied their final update on the Solarigate investigation with another blog post with recommendations for defending modern enterprise environments, titled Turning the page on Solarigate and opening the next chapter for the security community. Microsoft identified three key takeaways: adopt a Zero Trust mindset with an emphasis on protecting identities - especially privileged user accounts; embrace the cloud – specifically conducting identity access management from the cloud and not on premises; and strengthen the community of defenders – through working to share information on the Microsoft Security and Compliance Tech Community.
- FireEye is hosting a webinar titled Light in the Dark: Hunting for SUNBURST on February 25, live online 11:00 AM Eastern Time or after on demand. FireEye will present a first-ever look inside how Mandiant addressed the SUNBURST supply chain threat with customers, including stories from the front lines of the response efforts. The discussion will include: How this prolific cyber attack changes the way we view security; SUNBURST threat actor TTPs and how Mandiant hunts for the most relevant, and dangerous threats; and what threat hunting techniques should be deployed to find today’s stealthiest attackers. Registration is free and open to the public.

Technical Updates for February 8-12:

- CISA published Malware Analysis Report AR21-039A (MAR-10318845-1.v1 – SUNBURST) which provides detailed analysis of malicious artifacts associated with the SolarWinds compromise, identified by FireEye as SUNBURST. After being delivered as part of certain SolarWinds updates, a trojanized version of the “solarwinds.orion.core.businesslayer.dll” containing SUNBURST malware is installed by a legitimate SolarWinds installer application. The modified dynamic-link library (DLL) contains an obfuscated backdoor that allows a remote operator to execute functions on the compromised system, deploy additional payloads, and exfiltrate data. The
embedded SUNBURST code encrypts its outbound communications to the remote operator using XOR encryption and modified Base64 encoding. To avoid detection by security tools, the SUNBURST code will not run if it detects certain security software running on the target system. For a downloadable copy of IOCs, see: MAR-10318845-1.v1.stix.

- CISA also published Malware Analysis Report AR21-039B (MAR-10320115-1.v1 – TEARDROP) which provides detailed analysis of malicious artifacts associated with the SolarWinds compromise, identified by FireEye as TEARDROP. TEARDROP is a loader designed to decrypt and execute an embedded payload on the target system. The payload has been identified as the Cobalt Strike Beacon Implant (Version 4), which provides a remote operator with command and control capabilities over a victim system through an encrypted network tunnel. The capabilities include the ability to rapidly exfiltrate data, log keystrokes, take screenshots, and deploy additional payloads. For a downloadable copy of IOCs, see: MAR-10320115-1.v1.stix.

- Microsoft has released a questions and answers style blog post that delves into Microsoft’s response to Solorigate, their role in the investigation, and some other common questions they’ve received concerning the SolarWinds hack. One of the questions the blog addresses is the allegations made by other hacked companies that the attackers entered their systems or gained privileged credentials using Microsoft products as a vector. Microsoft staunchly denies these claims stating that while data hosted in Microsoft services (including email) were a target of the incident, the attacker gained privileged credentials some other way.

Technical Updates for February 1-5:

- Trustwave, a cybersecurity firm that focuses on threat detection and response, announced in their blog that they have discovered three security issues within SolarWinds products that can be characterized as “severe”. Two of the vulnerabilities impact the SolarWinds Orion Platform (CVE-2021-25274 and CVE-2021-25275) and one vulnerability impacts SolarWinds Serv-U FTP for Windows (CVE-2021-25276). The most critical vulnerability (CVE-2021-25274) allows for remote code execution with high privileges. None of the vulnerabilities are believed to have been exploited during the recent SolarWinds campaign. SolarWinds has been notified of the vulnerabilities and has provided patch updates for customers to install. Trustwave suggests that SolarWinds users install the patches as soon as possible as they plan to update the blog post with proof of concept (PoC) exploitation code on February 9. Trustwave has also included a fact sheet that provides more information about the discovered vulnerabilities.

- Cisco Talos blog posted a podcast episode titled Talos Takes Ep. #39: An update on SolarWinds as it relates to IoT and OT, which approaches the SolarWinds breach from an internet-of-things and operational security perspective. The guest speaker recently co-wrote a blog post for Cisco detailing how outsourcing OT over the past few years has made the SolarWinds compromise worse, and this podcast episodes expands on that blog post. The podcast discusses what we still don’t know about this attack, what you should do if you think you may be affected, and how we can learn from this going forward.

- SolarWinds updated their security advisory to include new information on the SUPERNOVA malware strain. SUPERNOVA is malware that was deployed using a vulnerability in the Orion Platform, and after the Orion Platform had been installed. The update notes that SUPERNOVA is not malicious code embedded within the builds of our Orion Platform as a supply chain attack. It is malware that is separately placed on a server that requires unauthorized access to a
customer’s network and is designed to appear to be part of a SolarWinds product. Additionally, the update notes that the SUPERNOVA malware consisted of two components. The first component was a malicious, unsigned webshell.dll specifically written to be used on the SolarWinds Orion Platform. The second is the utilization of a vulnerability in the Orion Platform to enable deployment of the malicious code. According to SolarWinds, this vulnerability in the Orion Platform has been resolved in the latest updates.

- SolarWinds is hosting a webinar titled Secure by Design: Our Plan for a Safer SolarWinds and Customer Community. Over the course of two sessions (February 4, 9 AM and 7 PM EST), the SolarWinds President and CEO Sudhakar Ramakrishna and cybersecurity expert and Krebs Stamos Group Founding Partner Alex Stamos will hold a discussion conversation on the company’s plan for a safer SolarWinds and customer community – grounded in key principles you can follow to secure your enterprise: Further secure the SolarWinds internal environment, enhance the SolarWinds product development environment, ensure the security and integrity of SolarWinds software. Additionally, the discussion will educate the audience on how to audit your cloud trust relationships, learn to build for code integrity, learn to centralize your monitoring to accelerate detection and speed response, learn to document network dependencies to better control access, and learn to enhance permission rules and risk-based authentication.

- SANS Institute is hosting a Lightning Summit on the SolarWinds campaign on Thursday, February 04, 2021 at 12:00 PM EST. SANS instructors will present lightning talks summarizing some of the key lessons learned. During six 10-minute long talks, the audience will learn about the larger concern of supply chain attacks, how others have approached it (good and bad), what you may have missed about SolarWinds/Sunburst, what it means to have a trust compromise and how to recover, and how you are able to protect yourself or detect compromise.

Technical Updates for January 25-29:

- CISA published Malware Analysis Report AR21-027A (MAR-10319053-1.v1 – Supernova) which provides detailed analysis of several malicious artifacts affecting the SolarWinds Orion product, identified by the security company FireEye as SUPERNOVA. According to a SolarWinds advisory, SUPERNOVA is not embedded within the Orion platform as a supply chain attack; rather, it is placed by an attacker directly on a system that hosts SolarWinds Orion and is designed to appear as part of the SolarWinds product. CISA's assessment is that SUPERNOVA is not part of the SolarWinds supply chain attack described in Alert AA20-352A. The report describes the analysis of a PowerShell script that decodes and installs SUPERNOVA, a malicious webshell backdoor. The SUPERNOVA malware allows a remote operator to dynamically inject C# source code into a web portal provided via the SolarWinds software suite. The injected code is compiled and directly executed in memory. For a downloadable copy of IOCs, see: MAR-10319053-1.v1.stix.

- Qualys published a blog post noting that the malicious code is part of the OrionImprovementBusinessLayer class which is executed by creating a thread to avoid interrupting the regular flow of the dll. The code to create thread was part of RefreshInternal method, which is an infected method of the dll. Qualys notes that the TTPs which the attackers have used in this breach including, but not limited to: Supply Chain Compromise, Data Encoding,
Impair Defenses and Dynamic Resolution. Instead of doing major damage to the infected system, the attackers have focused on staying unnoticed from security products.

- SolarWinds released a security advisory discussing their new digital code-signing certificate. SolarWinds signs each of their software builds with a digital code-signing certificate as a mechanism for customers to validate the authenticity of the software. In response to the recent hack, the company is revoking the original certificate and re-signing and re-releasing all the products signed with the original certificate. To ensure continued performance of SolarWinds products, customers must upgrade to these versions before March 8, 2021. For those customers who cannot update by the March 8 deadline, SolarWinds has created a temporary script that will protect customer environments from the SUPERNOVA malware.
- Microsoft announced on Twitter that they will be holding a Microsoft 365 Defender public webinar on January 28th that will discuss the ongoing investigation and response to the Solorigate attack. Presenters will review how M365 Defender can detect various stages of Solorigate and assist with formulating response plans.

Technical Updates for January 18-22:

- Symantec published a blog update titled SolarWinds: How Sunburst Sends Data Back to the Attackers. The post discussed how the SUNBURST malware used steganography - the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection. In this process, if data is being sent to the attacker as a result of a command, instead of performing a HTTP(S) GET request, Sunburst initiates a HTTP(S) POST request. The encrypted data to send is broken into multiple variable sized chunks. On receipt, the attacker will need to decode and concatenate all the message chunks, skipping junk chunks where the Timestamp second bit is not set.
- The Zero Day Initiative security blog posted an update titled Three Bugs in Orion’s Belt: Chaining Multiple Bugs for Unauthenticated RCE in the SolarWinds Orion Platform. The blog post details a few recently patched vulnerabilities in the SolarWinds Orion Platform and includes a useful youtube video demonstrating how the vulnerabilities can be exploited. When combined, these bugs can be exploited by an unauthenticated attacker to execute arbitrary code as Administrator on an affected system. One of these vulnerabilities, CVE-2020-14005, has been linked to the recent SUNBURST cyberattack on SolarWinds. However, the exact details around how, or if, this specific bug was used in the wild are still unclear.
- Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center, and Microsoft Cyber Defense Operations Center published a joint blog update titled Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop. In the update, Microsoft identifies the missing link in the complex Solorigate attack chain, the handover from the Solorigate DLL backdoor to the Cobalt Strike loader. The investigation shows that the attackers went out of their way to ensure that these two components are separated as much as possible to evade detection. The update provides details about this handover based on a limited number of cases where this process occurred.
- Microsoft Security Team published a blog update titled Using Zero Trust principles to protect against sophisticated attacks like Solorigate. The post discusses the implementation of the Zero Trust framework in practical terms, including: explicit access verification, ensuring least privilege access, shifting to an assumed breach mindset, and enabling multi-factor authentication. Additionally, zero trust principles rely on contextual real-time policy
enforcement to minimize risks, while using automation and machine learning to enable rapid
detection, prevention, and remediation.

- FireEye has released a blog update which includes a white paper titled Remediation and
Hardening Strategies for Microsoft 365 to Defend Against UNC2452. The white paper is an in-
depth detailing of initial compromise techniques along with detection, remediation, and
hardening strategies that companies can apply. Additionally, FireEye also released a free tool on
GitHub named Azure AD Investigator which they claim will assist companies with determining if
the SolarWinds hackers have used any of the identified techniques on their networks.

- Malwarebytes, a cybersecurity firm, revealed that it was hacked by the same threat actors that
hacked SolarWinds. The company stated that the attack was not related to the original supply
chain attack as they don’t use SolarWinds products within its internal networks. Instead, they
were notified by Microsoft Security Response Center (MSRC) that there was an intrusion that
exploited an Azure Active Directory weakness. An investigation determined that the attackers
only gained access to a “limited subset of internal company emails”. Malwarebytes also
conducted a thorough audit of their product and source code to ensure there were no signs of
compromise. The CEO stated that their investigation shows no evidence of unauthorized access
or compromise, that no user data was compromised, and that their software remains safe to
use.

- Symantec threat hunter team published a blog update on a fourth strain of malware used in the
SolarWinds breach, called Raindrop. The Raindrop malware, a loader which delivers a payload of
Cobalt Strike, was used against a select number of victims that were of interest to the attackers.
According to Symantec, Raindrop is very similar to the already documented Teardrop tool, with
some key differences. While Teardrop was delivered by the initial Sunburst backdoor, Raindrop
appears to have been used for spreading across the victim’s network. Symantec reports having
seen no evidence to date of Raindrop being delivered directly by Sunburst. Instead, it appears
elsewhere on networks where at least one computer has already been compromised by
Sunburst.

Technical Updates for January 11-15:

- CISA released AR21-013A Strengthening Security Configurations to Defend Against Attackers
Targeting Cloud Services, addressing several recent successful cyber-attacks. The report details
the tactics, techniques, and procedures, such as phishing, used by threat actors as well as
indicators of compromise to be aware of. The analysis also contains recommended mitigations
organizations can use to strengthen their cloud environment configuration in order to protect,
deter, and respond to potential attacks.

- Microsoft has launched a dedicated resiliency site for users of Microsoft 365 and Azure in
response to the ongoing SolarWinds breach. The Microsoft 365 Defender Team provides
security posture recommendations, based upon insights and analysis gained as a result of the
breach that can be implement immediately to improve network security.

- Kaspersky, a cybersecurity firm, released a new analysis of the SolarWinds breach and revealed
several similarities in the SUNBURST code that overlap with Kazaur, a previously reported
malware. Kazaur is believed to be developed by a Russian hacking group called Turla in 2017 and
first reported on by Palo Alto. In their analysis, Kaspersky explores several possible explanations
for the similarities in the code while noting the actor behind SolarWinds is still unknown. Their
analysis encourages other cybersecurity researchers to examine the overlap in the continued
efforts of investigating and analyzing the SolarWinds breach.

- CrowdStrike, a cyber security firm working in conjunction with SolarWinds Inc. regarding the
  breach, has released a new technical analysis that provides new insight into the build process by
  identifying a new strain of malware used in the attack. The newly identified malware, SUNSPOT,
  was the first used by the unknown adversary to watch the Orion build process and replace
  source code files with the SUNBURST malware when possible.

- CISA has released AA21-008A Detecting Post-Compromise Threat Activity in Microsoft Cloud
  Environments, a companion alert to AA20-352A Advanced Persistent Threat Compromise of
  Government Agencies, Critical Infrastructure, and Private Sector Organizations. This new alert
  presents evidence gathered by CISA of an advance persistent threat actor (APT) in the cloud
  environment, specifically using compromised applications in Microsoft 365/Azure. The alert also
details the use additional credentials and Application Programming Interface (API) access to
  cloud resources. The alert describes the malicious APT activity and also provides open-source
  tools to mitigate risk and compromise, including SPARROW – the CISA tool that helps users
  detect malicious activity that is a part of the ongoing SolarWinds compromise.

- FIREYE’s Mandiant Team, the team who uncovered the SolarWinds supply chain attacks, is
  hosting a webinar on January 12th. The webinar, UNC2452: What We Know So Far, will be focus
  upon sharing intelligence and information that FIREYE has compiled regarding the threat actor
  behind the attacks.

Technical Updates for January 4-8:

- Microsoft released a blog update disclosing that the Solarigate threat actors accessed an
  unspecified number of source code repositories. Microsoft stated: “Our investigation into our
  own environment has found no evidence of access to production services or customer data.
The investigation, which is ongoing, has also found no indications that our systems were used
to attack others.” Microsoft noted their inner source approach - the use of open source
  software development best practices and an open source-like culture.

- Yesterday evening, on behalf of the Cyber Unified Coordination Group, CISA published a Joint
  Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure
  Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the
  National Security Agency (NSA). The joint statement attributed the SolarWinds/SUNBURST
  incident to “an Advanced Persistent Threat (APT) actor, likely Russian in origin.” An excerpt of
  the joint statement can be found below, and the full text can be found on the CISA webpage.

- CISA has released Emergency Directive 21-01 Supplemental Guidance V.3, which requires
  agencies who ran affected versions of SolarWinds Orion software to conduct forensic analysis,
  agencies who accept the risks of running SolarWinds Orion software comply with certain
  hardening requirements, and reporting by agency from department-level Chief Information
  Officers (CIOs) by Tuesday, January 19th, and Monday, January 25th.

- In addition to 21-01 V.3, CISA also released updates to AA20-352A: Advanced Persistent
  Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector
  Organizations. The update includes new information on the initial access vectors, updated
  mitigation recommendations, and new indicators of compromise (IOCs). CISA has evidence
  there are initial access vectors other than SolarWinds Orion and has identified legitimate
  account abuse as one of these vectors. CISA is investigating incidents where impacted
SolarWinds instances have not been identified but Security Assertion Markup Language (SAML) tokens consistent with this adversary’s behavior are present. This alert will continue to be updated as CISA identifies changes to the tactics, techniques and procedures (TTPs) and confirms initial access vectors.

Technical Updates for December 28-January 3:

- CISA has released [Emergency Directive 21-01 Supplemental Guidance V.2](https://www.cisa.gov/sites/default/files/documents/2021-01/emergency-directive-21-01-supplemental-guidance-v-2-001.pdf), which instructs all federal agencies operating versions of SolarWinds Orion platform other than “affected versions” to ensure they update to SolarWinds Orion Platform version 2020.2.1HF2 by COB on December 31st. This version has been examined by the NSA to verify it eliminates the previously identified malicious code. SolarWinds Orion platforms 2019.4 HF5, 2020.2 RC1, 2020.2 RC2, 2020.2, 2020.2 HF1 should remain powered down and removed from networks.
- Microsoft published [Using Microsoft 365 Defender to protect against Solorigate](https://blogs.msdn.microsoft.com/security/2020/12/24/using-microsoft-365-defender-to-protect-against-solorigate/), what they are presenting as a comprehensive guide for security operations and incident response teams using Microsoft 365 Defender to identify, investigate, and respond to the Solorigate attack if it is found in your environment. The blog post covers: the Solorigate attack chain, reviewing affected devices and related incidents with threat analytics, detecting and blocking malicious activity on endpoint, detecting hands-on-keyboard activity within on-prem environment detecting hands-on-keyboard activity in the cloud environment, and a summary of detections and hunting queries across Microsoft 365 Defender.

Technical Updates for December 21-27:

- [CISA created a free tool](https://www.cisa.gov/otd/protecting-cloud-infrastructure-tools-for-detecting-unusual-and-potentially-malicious-activity-in-an-azure-microsoft-o365-environment) for detecting unusual and potentially malicious activity that threatens users and applications in an Azure/Microsoft O365 environment. The tool is intended for use by incident responders and is narrowly focused on activity that is endemic to the recent identity- and authentication-based attacks seen in multiple sectors. CISA strongly encourages users and administrators to visit the following [GitHub page](https://github.com/cisagov/azure-monitoring-tool) for additional information and detection countermeasures.
- [CISA released](https://www.cisa.gov/otd/protecting-cloud-infrastructure-tools-for-detecting-unusual-and-potentially-malicious-activity-in-an-azure-microsoft-o365-environment) Insights and new CISA webpage for consolidated guidance on this supply chain compromise, as reference points for information on the impact of the SolarWinds/SUNBURST compromise impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations.
- The CERT Communications Center at Carnegie Melon published [Vulnerability Note VU#843464: SolarWinds Orion API authentication bypass allows remote command execution](https://www.cisa.gov/sites/default/files/documents/2020-12/vulnerability-note-vu843464-solarwinds-orion-api-authentication-bypass-allows-remote-command-execution.pdf), which described how the Orion API is vulnerable to authentication bypass that could allow a remote attacker to execute API commands.
- [FireEye published](https://www.fireeye.com/blog/threat-research/2020/12/additional-technical-details-sunburst-backdoor.html) Additional Technical Details about the SUNBURST backdoor since their initial publication on Dec. 13, 2020. The update covers the following topics in greater detail: Anti-Analysis Environment Checks and Blocklists, Domain Generation Algorithm and Variations, Command and Control (C2) behaviors for DNS A and CNAME records, Malware modes of operation.
An Israeli cybersecurity firm published Detection and Hunting of Golden SAML Attack. The report notes that a technique used by the SolarWinds attackers was compromising the Security Assertion Markup Language (SAML) signing certificate, using their Active Directory privileges. The “Golden SAML” attack technique enables attackers to forge SAML responses and bypass ADFS authentication to access federated services. First reported by CyberArk in 2017, the current attack is the first time that this technique is known to have been used “in the wild”.

The Congressional Research Service released an initial assessment of the SolarWinds incident, titled SolarWinds Attack—No Easy Fix. The document discussed the attack, federal actions to date, and cybersecurity policy considerations for future risk management, incident response and remediation.

Symantec has released their first follow-up analysis on the SolarWinds Hack, detailing how the attack was carried out and the attackers avoided detection. Symantec has not reported any of their systems affected by the hack.

Technical Updates for the week of December 18-20:

- CISA has updated AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, originally released December 17. CISA has evidence of, and is currently investigating, initial access vectors in addition to those attributed to the SolarWinds Orion supply chain compromise. This update also provides new mitigation guidance, revises the indicators of compromise table, and includes a downloadable STIX file of the IOCs.
- CISA has released supplemental guidance to Emergency Directive (ED) 21-01, providing new information on affected versions, new guidance for agencies using third-party service providers, and additional clarity on required actions.
- Cisco Talos Blog was updated to verify the name server for the DGA domain was updated as far back as late February.
- Microsoft 365 Defender Research Team and the Microsoft Threat Intelligence Center published Analyzing Solorgiategate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers.
- CISA released a quick sheet for reference, soft copy available upon request.
- CISA released additional technical details, IOCs: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- NSA releases update on Detecting Abuse of Authentication Mechanisms
- SolarWinds is maintaining an up-to-date security advisory. As of December 17th, SolarWinds has removed all software builds affected by SUNBURST from download sites.
- FireEye published a series of tweets that in collaboration with GoDaddy and Microsoft, the organizations have identified a kill switch for SUNBURST and overtaken avsvmcloud[.]com. to server the malware and prevent new intrusions.
- Palo Alto Unit42 published a blog update: SUPERNOVA: SolarStorm’s Novel .NET Webshell Trojanized SUNBURST software with a certificate issued by Symantec has been discovered. Symantec has since clarified that the certificate was sold to Digicert in 2018 and was using a legacy certificate. Digicert is investigating the breach. At this time, Symantec software and business systems are not affected.